

Application No. 10730167 (Docket: CNTR.2224-C1)
37 CFR 1.111 Amendment dated 08/04/2007
Reply to Office Action of 04/23/2007

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0019] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, ~~an instruction is provided for employment by a device~~ a microprocessor apparatus is provided, for performing a cryptographic operation. ~~The instruction directs the device to perform a cryptographic operation.~~ The microprocessor apparatus includes fetch logic that is configured to fetch an instruction flow from memory for execution by a microprocessor. The instruction flow includes an instruction that directs the microprocessor to perform the cryptographic operation. The instruction has an opcode field and a repeat prefix field. The opcode field prescribes that the device accomplish the cryptographic operation as further specified within a control word stored in a memory. The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the instruction is to be accomplished on a plurality of blocks of input data.

[0021] Another aspect of the present invention provides an apparatus for performing cryptographic operations. The apparatus has fetch logic, that fetches an instruction flow from memory for execution by a microprocessor. The instruction flow includes a cryptographic instruction ~~that is received by logic within a circuit~~, where the cryptographic instruction prescribes one of the cryptographic operations. The cryptographic instruction includes an opcode field and a repeat prefix field. The opcode field prescribes that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory. The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data.